

CLAIM AMENDMENTS

1. (Currently Amended) A method for use in a device coupled to a communications channel, comprising:

determining a security service to perform with a data block;

generating security information to pass along with the data block, the security information identifying the security service; and

using a computer peripheral device adapted to control communication with the communications channel to select the security service from other security services based on the security information; and

processing, in [[a]] the computer peripheral device ~~adapted to control communication with the communications channel~~, the data block according to the security information.

2. (Original) The method of claim 1, wherein the processing includes performing cryptographic processing of the data block.

3. (Original) The method of claim 1, further comprising:

receiving the data block from a software routine; and

routing the processed data block back to the software routine after processing.

4. (Previously Presented) The method of claim 1, further comprising:

determining if the security service can be performed by the computer peripheral device; and

if not, processing the data block according to the security service in a software routine instead of the computer peripheral device.

5. (Original) The method of claim 1, further comprising identifying a security service according to an Internet Protocol security protocol.

6.-12. (Cancelled)

13. (Previously Presented) An article including a machine-readable storage medium containing instructions for execution in a system including a computer peripheral device adapted to control communications with a communications channel, the instructions when executed causing the system to:

receive a data block from the computer peripheral device;

determine from information in the data block if a security service has been performed on the data block by the computer peripheral device; and

process the data block if the security service has not been performed on the data block by the computer peripheral device.

14. (Previously Presented) The article of claim 13, the storage medium containing instructions that when executed causes the system to retrieve security information associated with the data block and send the data block and security information to the computer peripheral device to perform the security service.

15. (Original) The article of claim 13, the storage medium containing instructions that when executed causes the system to perform the security service on the data block.

16. (Currently Amended) A controller for controlling communications with a transport medium, the controller comprising:

a receiving circuit to receive data and associated security control information, the security control information identifying a security service to be performed on the data; and

a cryptographic engine to select the security service from other security services based on the security control information and cryptographically process the data based on the security control information selection, the cryptographic engine being a computer peripheral device.

17. (Original) The controller of claim 16, further comprising a storage device containing information identifying security services to be performed, the received security control information selecting a portion of the security services information in the storage device, wherein the cryptographic engine processes the data according to the selected portion of the security services information.

18. (Original) The controller of claim 17, further comprising a device adapted to change the contents of the storage device to update the security services information.

19. (Original) The controller of claim 18, wherein the device is adapted to update the security services information based on a predetermined replacement policy.

20. (Original) The controller of claim 17, wherein the security services information includes security association information.

21.-27. (Cancelled)

28. (Previously Presented) A method for use in a device coupled to a communications channel, comprising:

determining a security service to perform with a data block;

generating security information to pass along with the data block, the security information identifying at least one of an encryption algorithm and an authentication algorithm to be performed by the security service; and

processing, in a computer peripheral device adapted to control communication with the communications channel, the data block according to the security information.

29. (Previously Presented) The method of claim 28, wherein the processing includes performing cryptographic processing of the data block.

30. (Previously Presented) The method of claim 28, further comprising:
receiving the data block from a software routine; and
routing the processed data block back to the software routine after processing.
31. (Previously Presented) The method of claim 28, further comprising:
determining if the security service can be performed by the computer peripheral device; and
if not, processing the data block according to the security service in a software routine instead of the computer peripheral device.
32. (Previously Presented) The method of claim 28, further comprising identifying a security service according to an Internet Protocol security protocol.
33. (Previously Presented) A controller for controlling communications with a transport medium, the controller comprising:
a receiving circuit to receive data and associated security control information, the security control information identifying at least one of an encryption algorithm and an authentication algorithm to be performed on the data; and
a cryptographic engine to cryptographically process the data based on the security control information, the cryptographic engine being a computer peripheral device.
34. (Previously Presented) The controller of claim 33, further comprising a storage device containing information identifying security services to be performed, the received security control information selecting a portion of the security services information in the storage device, wherein the cryptographic engine processes the data according to the selected portion of the security services information.
35. (Previously Presented) The controller of claim 34, further comprising a device adapted to change the contents of the storage device to update the security services information.

36. (Previously Presented) The controller of claim 35, wherein the device is adapted to update the security services information based on a predetermined replacement policy.

37. (Previously Presented) The controller of claim 34, wherein the security services information includes security association information.